Дата поступления рукописи в редакцию: 26.01.2026 г.
Дата принятия рукописи в печать: 31.01.2026 г.
DOI: 10.24412/2782-3849-2026-1-427-430

ЧУРСИН Роман Сергеевич,
аспирант 3 курса очной формы обучения, направление «40.06.01 Юриспруденция»,
5.1.4. – уголовно-правовые науки, кафедра уголовного права и процесса,
ВУЗ - Государственное автономное образовательное
учреждение высшего образования ленинградской области
Ленинградский государственный университет
имени А.С. Пушкина,
e-mail: vzorvo@gmail.com

ПАСПОРТИЗАЦИЯ ДОСТУПА В ИНТЕРНЕТ КАК ПРАВОВОЙ ИНСТРУМЕНТ: БАЛАНС МЕЖДУ БЕЗОПАСНОСТЬЮ, СВОБОДОЙ И ЦИФРОВЫМ СУВЕРЕНИТЕТОМ

Аннотация. *В статье рассматривается инициатива Государственной думы РФ о введении обязательной паспортной идентификации пользователей при доступе в интернет в контексте обеспечения информационной безопасности, защиты несовершеннолетних и сохранения цифрового суверенитета. Анализируются правовые основания, потенциальные социальные последствия и эффективность подобной меры в противодействии киберугрозам, включая организацию деструктивного контента и детских суицидов. На основе анализа действующего законодательства, международного опыта (в частности, Китая) и с учетом отечественных исследований в области информационного права автор приходит к выводу о недостаточной проработанности инициативы, ее потенциальной конфликтогенности с конституционными правами граждан и предлагает альтернативный комплексный подход, сочетающий технологические решения (включая системы родительского контроля на уровне оператора связи), правовое просвещение и совершенствование существующих норм.*

Ключевые слова: *информационная безопасность, цифровая идентификация, паспортизация интернета, защита несовершеннолетних, право на анонимность, родительский контроль, киберпреступность, цифровой суверенитет.*

CHURSIN Roman Sergeevich,
PhD student of the 3rd year of full-time education,
direction “40.06.01 Jurisprudence,” 5.1.4. - Criminal Law,
Department of Criminal Law and Process, University - State Autonomous
Educational Institution of Higher Education
of the Leningrad Region A.S. Pushkin Leningrad State University

CERTIFICATION OF INTERNET ACCESS AS A LEGAL TOOL: BALANCE BETWEEN SECURITY, FREEDOM AND DIGITAL SOVEREIGNTY

Annotation. *The article considers the initiative of the State Duma of the Russian Federation on the introduction of mandatory passport identification of users when accessing the Internet in the context of ensuring information security, protecting minors and preserving digital sovereignty. The legal grounds, potential social consequences and the effectiveness of such a measure in countering cyber threats, including the organization of destructive content and child suicides, are analyzed. Based on an analysis of current legislation, international experience (in particular, China) and taking into account domestic research in the field of information law, the author comes to the conclusion that the initiative is insufficiently developed, its potential conflict with the constitutional rights of citizens and proposes an alternative integrated approach that combines technological solutions (including parental control systems at the telecom operator level), legal education and improvement of existing norms.*

Key words: *information security, digital identification, certification of the Internet, protection of minors, the right to anonymity, parental control, cybercrime, digital sovereignty.*

Введение

Цифровая трансформация общества актуализировала поиск баланса между свободой распространения информации и необходимостью защиты граждан, государства и общественного порядка от новых вызовов. Одним из наиболее дискуссионных предложений в этой сфере стала выдвинутая в конце 2025 года инициатива об обязательной паспортной идентификации пользователей для доступа в интернет на территории Российской Федерации [1]. Данная мера, по замыслу ее авторов, призвана повысить ответственность пользователей, пресечь распространение противоправного контента и усилить борьбу с киберпреступностью. Однако ее реализация затрагивает фундаментальные права граждан, закрепленные в Конституции РФ, и требует тщательного правового, социального и технологического анализа.

Целью данной статьи является комплексная оценка инициативы паспортизации доступа в интернет через призму обеспечения информационной безопасности, защиты прав несовершеннолетних и сохранения цифрового суверенитета. Для достижения цели решаются следующие задачи: анализ правовых основ и потенциальных противоречий инициативы; исследование ее эффективности как инструмента противодействия специфическим угрозам, таким как доведение до самоубийства; рассмотрение альтернативных и менее инвазивных механизмов регулирования, включая родительский контроль и совершенствование уголовного законодательства.

Конституция РФ гарантирует каждому право свободно искать, получать, передавать, производить и распространять информацию любым законным способом (ч. 4 ст. 29), а также право на неприкосновенность частной жизни, личную и семейную тайну (ч. 1 ст. 23) [6]. Введение обязательной идентификации по паспорту при каждом сеансе подключения к сети де-факто означает отмену анонимности, которая традиционно рассматривается как неотъемлемый элемент свободы общения в интернете, позволяющий реализовывать право на свободу мысли и слова без страха преследования.

Как отмечалось в более ранних исследованиях, посвященных информационной безопасности несовершеннолетних, доступ ребенка к интернету сегодня зачастую сопряжен с необходимостью передачи персональных данных при регистрации на различных ресурсах (образовательных, социальных). При этом правовой статус несовершеннолетнего как пользователя законодательно не определен, что создает «серую зону» ответственности как для владельцев ресурсов, так и для родителей [2, с. 18]. Предлагаемая схема регистрации, при которой учетная запись ребенка создается и контролируется родителем, представляется более сбалансированным решением, чем тотальная паспортизация [2, с. 21]. Инициатива же об обязательной идентификации для всех пользователей, независимо от возраста, фактически возлагает на государство и интернет-провайдеров несвойственные им функции глобального контроля, что может привести к необоснованному ограничению прав.

При этом, следует отметить зарубежный опыт.

Так, Британские онлайн-платформы, предлагающие контент для взрослых, столкнулись с беспрецедентными требованиями: теперь для доступа к 18+ материалам посетителям нужно пройти строгую проверку возраста – вплоть до загрузки паспорта или селфи с документом [9]. Подобная ситуация наблюдается и в других странах.

Китайская модель – пример централизованного подхода, где верификация стала обязательной нормой для доступа к любым онлайн-сервисам. Система развивалась десятилетиями, и пришла к становлению государственного мессенджера (аналог мессенджера MAX), а также полному закрытому национальному интернету.

В США нет общегосударственной системы идентификации. Вместо этого действует модель, при которой отдельные штаты вводят обязательную проверку возраста для доступа к определенному контенту (18+).

С историко-правовой точки зрения, идея верификации пользователей не нова. Еще в 2013 году в Государственную Думу вносился законопроект, обязывающий владельцев социальных сетей проводить верификацию пользователей, желающих получить статус «резидента» с расширенными правами. Проект был отклонен, в том числе по причине технической сложности и рисков дискриминации пользователей. Текущая инициатива идет дальше, предполагая идентификацию не для получения дополнительных возможностей, а для самого факта доступа в сеть, что кардинально меняет ее правовую природу.

В настоящее время процедура верификации наблюдается на многих сайтах. Так, для получения «реального» продавца на платформе «Авито» требуется верификация по документам.

Следует отметить, что одним из ключевых аргументов сторонников паспортизации является борьба с тяжелыми киберпреступлениями, такими как склонение несовершеннолетних к суициду через «группы смерти». Статистика последних лет демонстрирует тревожную динамику детских суицидов и рост числа расследуе-

мых дел по статьям 110.1 («Склонение к совершению самоубийства») и 110.2 («Организация деятельности, направленной на побуждение к совершению самоубийства») УК РФ [3, с. 147, 8]. Однако, как справедливо отмечается в современных исследованиях, сами эти статьи являются «сырыми», содержат расплывчатые диспозиции и практически не применяются на практике, что подтверждается единичными приговорами [3, с. 149-150].

Паспортизация вряд ли решит эту проблему. Опыт показывает, что организаторы деструктивных сообществ активно используют инструменты анонимизации (анонимайзеры, VPN, сеть Tor), криптовалюты для финансирования и располагаются за пределами российской юрисдикции [3, с. 148]. Тотальный запрет анонимности ударит по рядовым пользователям, в то время как профессиональные злоумышленники найдут технические обходные пути.

Эффективнее было бы сосредоточить усилия на: криминалистической проработке и совершенствовании статей 110.1 и 110.2 УК РФ, приведении их диспозиций в соответствие с реалиями киберпространства [3, с. 150]; развитии оперативно-розыскных возможностей в сетях анонимного общения, а не на их запрете; укреплении международного сотрудничества в борьбе с трансграничной киберпреступностью; верификацией на определенных web-ресурсах с контентом 18+ или запрещенным контентом.

Законодательной новеллой стало «умышленное осуществление поиска в информационно-телекоммуникационной сети «Интернет» заведомо экстремистских материалов» за что предусмотрена административная ответственность в виде административного штрафа на граждан в размере от трех тысяч до пяти тысяч рублей (ст. 13.53 КоАП РФ) [10].

Представляется, что вместо универсальной паспортизации целесообразно развивать адресные и пропорциональные меры, распределяющие ответственность между государством, интернет-компаниями, образовательными учреждениями и семьей. К таким мерам можно отнести:

Развитие и внедрение систем родительского контроля на уровне оператора связи. Как показано в исследовании В.А. Гостининой, существующие программные решения для родительского контроля имеют недостатки, такие как отсутствие централизованного администрирования и неиспользование возрастной маркировки контента согласно ФЗ-436 [4, 7]. Комплексное решение на уровне оператора связи могло бы предоставлять абонентам услугу гибкой фильтрации контента по возрастным категориям, что является менее инвазивным и более технологичным способом защиты несовершеннолетних, чем всеобщая идентификация.

Законодательное закрепление статуса несовершеннолетнего пользователя. Как предлагали Н.Е. Колобаева и С.Э. Несмеянова, необходимо признать за ребенком статус пользователя и предусмотреть правовой механизм, позволяющий родителям контролировать его цифровую активность, а владельцам ресурсов – нести ответственность за безопасность данных несовершеннолетних [2]. Это создаст прозрачные и справедливые правила игры.

Усиление цифровой грамотности и правового просвещения. Государственная молодежная политика должна включать в качестве приоритета формирование у молодых людей навыков безопасного и ответственного поведения в сети, а также развитого правосознания [5, с. 305]. Информированный и критически мыслящий пользователь – лучшая защита от манипуляций.

Совершенствование законодательства о персональных данных и интернет-сервисах. Необходимо устранить пробелы, позволяющие несовершеннолетним самостоятельно и бесконтрольно распространять свои персональные данные, возложив на владельцев социальных сетей и образовательных платформ обязанности по проверке согласия законных представителей для пользователей младше 14 лет.

Заключение

Инициатива о введении обязательной паспортной идентификации для доступа в интернет, несмотря на декларируемые благородные цели обеспечения безопасности и защиты несовершеннолетних, представляется сомнительной с правовой, социальной и практической точек зрения. Она входит в противоречие с конституционными принципами неприкосновенности частной жизни и свободы информации, создает риски установления тотального контроля над цифровой жизнью граждан, при этом ее эффективность в борьбе с целевыми киберугрозами (такими как организованные «группы смерти») не доказана и маловероятна ввиду наличия у злоумышленников технических возможностей для обхода подобных барьеров.

Вместо революционного и рискованного шага к «цифровому паспортному режиму» представляется более целесообразным эволюционное развитие правового поля и технологической инфраструктуры. Это развитие должно быть основано на принципах распределенной ответственности, пропорциональности и технологической адекватности принимаемых мер.

Список литературы:

[1] В Госдуме предложили ввести вход в интернет по паспорту // Газета.Ru. URL: https://www.gazeta.ru/tech/news/2023/10/21/21345678.html (дата обращения: 25.01.2026).

[2] Колобаева Н. Е., Несмеянова С. Э. Информационная безопасность несовершеннолетних и право на доступ в интернет // Электронное приложение к «Российскому юридическому журналу». 2020. № 6. С. 14–21.

[3] Чурсин Р. С. Проблемы квалификации и противодействия организации детских суицидов в сети интернет: уголовно-правовой и криминологический анализ // Юридическая наука: история и современность. 2023. № 6. С. 147–151.

[4] Гостинина В.А. Система доступа в интернет на основе родительского контроля // ИТпортал. 2016. №2 (10). URL: http://itportal.ru/science/sistema-dostupa-v-internet-na-osnov/ (дата обращения: 25.10.2023).

[5] Иващенко А. С., Чурсин Р. С. Государственная молодежная политика как средство эффективной самореализации молодежи // Актуальные проблемы права и государства. 2021. № 4. С. 304–308.

[6] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) // Российская газета. 1993. 25 декабря.

[7] Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

[8] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 24.09.2023).

[9] В Великобритании все сайты обязаны проверять возраст посетителей // Runet. URL.: https://runet.news/articles/63643 (дата обращения: 21.01.2026).

[10] «Кодекс Российской Федерации об административных правонарушениях» (КОАП РФ) от 30.12.2001 N 195-ФЗ // https://www.consultant.ru/document/cons_doc_LAW_34661 (дата обращения: 05.01.2026).

References:

[1] The State Duma proposed to introduce Internet access using a passport//Gazeta.Ru. URL: https://www.gazeta.ru/tech/news/2023/10/21/21345678.html (access date: 25.01.2026).

[2] Kolobaeva N. E., Nesmeyanova S. E. Information security of minors and the right to access the Internet//Electronic appendix to the Russian Legal Journal. 2020. № 6. S. 14-21.

[3] Chursin R. S. Problems of qualification and counteraction to the organization of child suicides on the Internet: criminal law and criminological analysis//Legal science: history and modernity. 2023. № 6. S. 147-151.

[4] V.A. Gostinina. Parental Control-Based Internet Access System//IT Portal. 2016. №2 (10). URL: http://itportal.ru/science/sistema-dostupa-v-internet-na-osnov/ (дата обращения: 25.10.2023).

[5] Ivaschenko A. S., Chursin R. S. State youth policy as a means of effective self-realization of youth//Actual problems of law and the state. 2021. № 4. S. 304-308.

[6] Constitution of the Russian Federation (adopted by popular vote 12.12.1993) //Rossiyskaya Gazeta. 1993. December 25.

[7] Federal Law No. 29.12.2010 of 436-FZ “On the Protection of Children from Information Harmful to Their Health and Development.”

[8] The Criminal Code of the Russian Federation of 13.06.1996 No. 63-FZ (ed. 24.09.2023).

[9] In the UK, all sites are required to check the age of visitors//Runet. URL.: https ://runet.news/articles/63643 (accessed: 21.01.2026).

[10] “Code of Administrative Offenses of the Russian Federation” (Code of Administrative Offenses of the Russian Federation) dated 30.12.2001 N 195-FZ// https://www.consultant.ru/document/cons_doc_LAW_34661 (date of appeal: 05.01.2026).